

APPENDIX A

DEFINITIONS

1. Administrative purposes. Information is collected for "administrative purposes" when it is necessary for the administration of the component concerned but is not collected directly in performance of the intelligence activities assigned such component. Examples include information relating to the past performance of potential contractors; information to enable such components to discharge their public affairs and legislative duties, including the maintenance of correspondence files; the maintenance of employee personnel and training records; and training materials or documents produced at training facilities.

2. Available publicly. Information that has been published or broadcast for general public consumption, is available on request to a member of the general public, could lawfully be seen or heard by any casual observer, or is made available at a meeting open to the general public. In this context, the "general public" also means general availability to persons in a military community even though the military community is not open to the civilian general public.

3. Communications security. Protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government related to national security and to ensure the authenticity of such telecommunications.

4. Consent. The agreement by a person or organization to permit DoD intelligence components to take particular actions that affect the person or organization. Consent may be oral or written unless a specific form of consent is required by a particular procedure. Consent may be implied if adequate notice is provided that a particular action (such as entering a building) carries with it the **presumption** of consent to an accompanying action (such as search of briefcases). (Questions regarding what is adequate notice in **particular** circumstances should be referred to the legal office responsible for advising the DoD intelligence component concerned.)

5. Counterintelligence. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or international terrorist activities, but not including personnel, physical, document, or communications security programs.

6. Counterintelligence investigation. Includes inquiries and other activities undertaken to determine whether a particular United States person is acting for, or on behalf of, a foreign **power** for purposes of **conducting** espionage and other intelligence activities, sabotage, assassinations, international terrorist activities, and actions to neutralize such acts.

7. DoD Component. Includes the Office of the Secretary of Defense, each of the Military Departments, the Organization of the Joint Chiefs of Staff, the Unified and Specified Commands, and the Defense Agencies.

8. DoD intelligence components. Include the following organizations:
 - a. The National Security Agency/Central Security Service.
 - b. The Defense Intelligence Agency.
 - c. The offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs.
 - d. The Assistant Chief of Staff for Intelligence, Army **General** Staff.
 - e. The Office of Naval Intelligence.
 - f. The Assistant Chief of Staff, Intelligence, U.S. Air Force.
 - g. The Army Intelligence and Security Command.
 - h. The Naval Intelligence Command.
 - i. The Naval Security Group Command.
 - j. The Director of Intelligence, U.S. Marine Corps.
 - k. The Air Force Intelligence Service.
 - l. The Electronic Security Command, U.S. Air Force.
 - m. The counterintelligence elements of the Naval Investigative Service.
 - n. The **counterintelligence** elements of the Air Force Office of Special Investigations.
 - o. The 650th Military Intelligence Group, SHAPE.
 - p. Other organizations, staffs, and offices, when used for foreign intelligence or counterintelligence activities to which part 2 of **E.O. 12333** (reference (a)), applies, provided that the heads of such organizations, **staffs**, and offices shall not be considered as heads of DoD intelligence components for purposes of this Regulation.
9. Electronic surveillance. Acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a **nonelectronic** communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio direction finding equipment solely to determine the location of a transmitter. (Electronic surveillance within the United States is subject to the definitions in the Foreign Intelligence Surveillance Act of 1978 (reference (b)).)
10. Employee. A person employed by, assigned to, or acting for an agency within the intelligence community, including contractors and persons otherwise acting at the direction of such an agency.

11. Foreign intelligence. Information relating to the capabilities, intentions, and activities of foreign powers, organizations, or persons, but not including counterintelligence except for information on international terrorist activities.

12. Foreign power. Any foreign government (regardless of whether recognized by the United States), foreign-based political party (or faction thereof), foreign military force, foreign-based terrorist group, or any organization composed, in major part, of any such entity or entities.

13. Intelligence activities. Refers to all activities that DoD intelligence components are authorized to undertake pursuant to Executive Order 12333 (reference (a)).

14. Intelligence community and an agency of or within the intelligence community. Refers to the following organizations:

- a. The Central Intelligence Agency (CIA).
- b. The National Security Agency (NSA).
- c. The Defense Intelligence Agency (DIA).
- d. The Offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs.
- e. The Bureau of Intelligence and Research of the Department of State.
- f. The intelligence elements of the Army, Navy, Air Force and Marine Corps, the Federal Bureau of Investigation (FBI), the Department of the Treasury, and the Department of Energy.
- g. The staff elements of the Office of the Director of Central Intelligence.

15. International Narcotics Activities. Refers to activities outside the United States to produce, transfer or sell narcotics or other substances controlled in accordance with title 21, United States Code, Sections 811 and 812.

16. International Terrorist Activities. Activities undertaken by or in support of terrorists or terrorist organizations that occur totally outside the United States, or that transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which the perpetrators operate or seek asylum.

17. Lawful investigation. An investigation qualifies as a lawful investigation if the subject of the investigation is within DoD investigative jurisdiction; if it is conducted by a DoD Component that has authorization to conduct the particular type of investigation concerned (for example, counterintelligence, personnel security, physical security, communications security); and if the investigation is conducted in accordance with applicable law and policy, including E.O. 12333 and this Regulation.

18. Personnel Security. Measures designed to insure that person's employed, or being considered for employment, in sensitive positions" of trust are suitable for such employment with respect to loyalty, character, emotional stability, and reliability and that such employment is clearly consistent with the interests of the national security. It includes measures designed to ensure that persons granted access to classified information remain suitable for such access and that access is consistent with the interests of national security.

19. Personnel security investigation:

a. An inquiry into the activities of a person granted access to intelligence or other classified information; or a person who is being considered for access to intelligence or other classified information, including persons who are granted or may be granted access to facilities of DoD intelligence components; or a person to be assigned or retained in a position with sensitive duties. The investigation is designed to develop information pertaining to the suitability, eligibility, and trustworthiness of the individual with respect to loyalty, character, emotional stability and reliability.

b. Inquiries and other activities directed against DoD employees or members of a Military Service to determine the facts of possible voluntary or involuntary compromise of classified information by them.

c. The collection of information about or from military personnel in the course of tactical training exercises for security training purposes.

20. Physical security. The physical measures taken to prevent unauthorized access to, and prevent the damage or loss of, equipment, facilities, materiel and documents; and measures undertaken to protect DoD **personnel** from physical threats to their safety.

21. Physical security investigation. All inquiries, inspections, or surveys of the effectiveness of controls and procedures designed to provide physical security; and **all** inquiries and other actions undertaken to obtain information pertaining to physical threats to DoD personnel or property.

22. Reasonable belief. A reasonable belief arises when the facts and circumstances are such that a reasonable person would hold the belief. Reasonable belief must rest on facts-and circumstances that can be articulated; "hunches" or intuitions are not sufficient. Reasonable belief can be based on experience, training, and knowledge in foreign intelligence or **counterintelligence** work applied to facts and circumstances at hand, so that a trained and experienced "reasonable person" might hold a reasonable belief sufficient to satisfy this criterion when someone unfamiliar with foreign intelligence or counterintelligence work might not.

23. Signals intelligence. A category of intelligence including communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, either individually or in combination.

24. United States. When used to describe a place, the term shall include the territories under the sovereignty of the United States.

25. United States person.

a. The term "United States person" means:

(1) A United States citizen;

(2) An alien known by the DoD intelligence component concerned to be a permanent resident alien;

(3) An unincorporated association substantially composed of United States citizens or permanent resident aliens;

(4) A corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments. A corporation or corporate subsidiary incorporated abroad, even if partially or wholly owned by a corporation incorporated in the United States, is not a United States person.

b. A person or organization outside the United States shall be presumed not to be a United States person unless specific information to the contrary is obtained. An alien in the United States shall be presumed not to be a United States person unless specific information to the contrary is obtained. "

c. A permanent resident alien is a foreign national lawfully admitted into the United States for permanent residence.